v7.8.4 Release Notes for Websense® Content Gateway

Topic 60115 | Web Security Gateway and Gateway Anywhere | 26-Aug-2014

These Release Notes are an introduction to Websense Content Gateway version 7.8.4.

- *New in Websense Content Gateway v7.8.4*, page 2
- *Installation and upgrade*, page 7
- *Operating tips*, page 12
- *Resolved and known issues*, page 19

All sections of these notes include important information that helps ensure your successful installation, upgrade, and deployment of Content Gateway.

To find upgrade instructions for your Websense TRITON® solution, see:

- Upgrading TRITON Enterprise
- Upgrade Instructions: Web Security Gateway
- Upgrade Instructions: Web Security Gateway Anywhere

© 2015 Websense, Inc.

New in Websense Content Gateway v7.8.4

Topic 60116 | Web Security Gateway and Gateway Anywhere | 26-Aug-2014

Security

In some previous versions, the SSL module in Content Gateway included an OpenSSL version that includes the man-in-the-middle (MITM) vulnerabilities (CVE-2014-0224). Exploiting this vulnerability, an attacker that is capable of intercepting communications between a vulnerable client and server can exploit an MITM attack, allowing the attacker to transparently decrypt and modify traffic to and from both client and server. In version 7.8.4 of Websense Content Gateway, the vulnerable version of the OpenSSL libraries have been replaced with a fixed version.

Transparent Proxy supports IPv6

Support for IPv6 has been extended to transparent proxy deployments.

WCCP 2.01 is required to support IPv6. If you use a Cisco router, it must be version 15.4(1)T or later to support IPv6.

If Content Gateway is deployed on a Websense Appliance, IPv6 must be enabled on the **Configuration > Network Interfaces > IPv6** page of the Appliance Manager.

WCCP GRE Packet Forward Method and Packet Return Method and Dynamic bypass are not supported for IPv6 addresses.

IP spoofing requires all IPs in the routing path to use the same format. That is, all IPs must be IPV6 or IPv4. A combination of IPv6 and IPv4 is not supported.

Range based IP spoofing is not supported for IPv6.

IPv6 is not supported for FTP passive mode with the transparent proxy.

IPv6 only clients do not display a block page correctly. The user is blocked from the site as expected but will receive a browser error rather than a block page. Dual-stack IPv6 clients receive the normal block page.

In support of this feature, a new column for IPv6 data has been added to the ARM Statistics provided on the **Monitor > Networking > ARM** page.

Captive Portal enhancements

The new authentication method, Captive Portal, added to Content Gateway in v7.8.3, has been enhanced to provide support for:

- cookie authentication
- HTTPS portal

In version 7.8.3, credential caching and expiration was handled per the global configuration. Captive Portal has been enhanced to support cookie-based authentication with cookie-enabled applications (browsers) on mobile devices. Note that most applications on mobile devices do not share cookies. For those applications, IP-based identification will be required.

See Authentication using Captive Portal and the Credential Caching section of Global authentication options in Content Gateway Help for more information.

Note that for web applications that use Ajax where Ajax is configured to prevent cookies, cookie-mode cannot support sites that include cross-origin requests (CORS) that rely on Ajax.

Support for Captive Portal Authentication is enhanced to use HTTPS. When an authentication rule is configured to use Captive Portal and a user matches that rule, an HTTPS page prompts for credentials and the authentication transaction is handled with HTTPS.

When adding an authentication rule (see Rule-Based Authentication in Content Gateway Help for details), two options are now available to enable the Captive Portal feature. Navigate to **Configure > Security > Access Control > Authentication Rules** and, next to Captive Portal, click

- **Enabled for HTTPS Authentication page** to display the authentication page using HTTPS.

  When HTTPS is used, a server certification is generated based on the internal root CA. To use this feature, you must import the internal root CA to ensure there is no certificate error. See Importing your Root CA in Content Gateway Help for details.
- **Enabled for HTTP Authentication page** to display the authentication page using HTTP.
- **Disabled** to disable the feature.

When the feature is enabled, users who match the rule are redirected to the new web portal authentication page. See Authentication using Captive Portal in Content Gateway Help for more details.

Diagnostic tools available in Content Gateway manager

Automatic and manual diagnostics can now be run from **Monitor > My Proxy > Diagnostics** in Content Gateway manager.

Tests provided on the **Automatic** tab verify connectivity to:

- The IPv4 default gateway
- The IPv6 default gateway
- Your primary DNS server
- Your secondary DNS server
- download.websense.com (a Websense download server)
- ddsdom.websense.com (a Websense download server)
- ddsint.websense.com (a Websense download server)
- my.websense.com (customer account portal)

Click **Run Diagnostics** to view test results and latency information. Details for any test that failed or could not complete are provided. Results from the last test display each time the page is accessed and include the date and time of the test in the **Last update** information

The **Manual** tab offers 4 commands typically run from the command line.

- **Ping**, used to determine if a remote device can be reached across the network.
- **Traceroute**, used to determine the path network packets take and measure delays across the network.
- **NSlookup**, used to obtain domain name or IP address mapping.
- **TCPDump**, used to analyze network packets.

Select the command you wish to run, enter valid parameters, and click **Run** to execute the command. The results for Ping, Traceroute, and NSlookup display in a **Test Results** window provided on the page. The results for TCPDump are written to a file that can then be downloaded and viewed or saved using a link provided when the command completes. File size is limited to 10,000 packets to avoid disk space problems.

Platform Support

Note
IPv6 is not supported for FTP passive mode

Content Gateway runs on 64-bit platforms only.

Important
If you are planning to upgrade to version 7.8.4, and Content Gateway is currently hosted on a 5-series version of Red Hat Enterprise Linux, you must upgrade the operating system upgrade to Red Hat Enterprise Linux 6-series as part of the Content Gateway upgrade process. Red Hat Enterprise Linux 6.4 is recommended.

See Upgrading Websense Web Security solutions to find your upgrade procedure, which includes operating system upgrade instructions.

Content Gateway is certified on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.5: 2.6.32-431 (not recommended with v7.8.3 or later)
  - Kernel version for 6.4: 2.6.32-358
- V-Series appliances

Content Gateway is supported on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.3: 2.6.32-279
  - Kernel version for 6.2: 2.6.32-220
  - Kernel version for 6.1: 2.6.32-131
  - Kernel version for 6.0: 2.6.32-71
- The corresponding CentOS versions, including updates 3 and 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Only kernels listed above are certified or supported. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

Websense, Inc. provides “best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is

deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 7.8.4 Content Gateway installer.

Websense also recommends that Red Hat Enterprise Linux systems that host Content Gateway be registered with Red Hat Network and kept up-to-date with the latest security patches.

Important

You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel ABI.

Important

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

For a complete description of platform requirements, see *Hardware requirements* and *Operating system and software requirements*.

Installation and upgrade

Topic 60117 | Web Security Gateway and Gateway Anywhere | 26-Aug-2014

The Websense Deployment and Installation Center is the complete resource for deployment, installation, and upgrade information for version 7.8.4 TRITON Enterprise solutions.

Content Gateway is the proxy component of the Web Security Gateway and Web Security Gateway Anywhere solutions. **Installation and upgrade must be performed in the context of installation or upgrade of Web Security Gateway or Web Security Gateway Anywhere.**

> **Important**
> If you are using Content Gateway on a V-Series appliance, Content Gateway is installed when the appliance is factory imaged and upgraded with the appliance patch facility.

For complete installation information, see:

- Installing TRITON Enterprise
- Installation Instructions: Web Security Gateway
- Installation Instructions: Web Security Gateway Anywhere

For complete upgrade information, see:

- Upgrading TRITON Enterprise
- Upgrade Instructions: Web Security Gateway
- Upgrade Instructions: Web Security Gateway Anywhere

Below are summaries of Content Gateway:

- *Hardware requirements*
- *Operating system and software requirements*
- *Instructions for downloading the installer*

Hardware requirements

CPU	Quad-core running at 2.8 GHz or faster
Memory	6 GB minimum; 8 GB recommended
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data.

	• 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should have minimum size of 2 GB, maximum 147 GB for optimal performance – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – Should be, for best performance, a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache
Network Interfaces	2: • If not installed on an appliance, policy engine will fail to do auto-registration if there is no eth0 on the box.

To support transparent proxy deployments

Router	Must support WCCP v2, or Policy Based Routing (PBR). A Cisco router must run IOS 12.2 or later. To support IPv6, WCCP v2.01 and Cisco router version 15.4(1)T or later are required. Client machines, the destination Web server, and Websense Content Gateway must reside on different subnets.
—or—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). To support L2 forward or return, Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Operating system and software requirements

Red Hat Enterprise Linux

Content Gateway is certified on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.5: 2.6.32-431 (not recommended with v7.8.3 or later)

    - Kernel version for 6.4: 2.6.32-358
- V-Series appliances

Content Gateway is supported on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
    - Kernel version for 6.3: 2.6.32-279
    - Kernel version for 6.2: 2.6.32-220
    - Kernel version for 6.1: 2.6.32-131
    - Kernel version for 6.0: 2.6.32-71
- The corresponding CentOS versions, including updates 3 and 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Only kernels listed above are certified or supported. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

Websense, Inc. provides “best effort” support for the version of Red Hat Enterprise Linux and CentOS listed above. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

Websense recommends that the Red Hat Enterprise Linux version that will host Content Gateway be updated to the latest patch before running the version 7.8.4 Content Gateway installer.

Websense also recommends that Red Hat Enterprise Linux systems that host Content Gateway be registered with Red Hat Network and kept up-to-date with the latest security patches.

Important

You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel ABI.

Important

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

Websense Web Security Gateway / Anywhere

- Version 7.8.4 required

> **Important**
> Web Security Policy Server and Filtering Service must be installed before Content Gateway.

Websense Data Security

- Version 7.8.4
- Any version can be used via the ICAP interface. See the Content Gateway Manager Help for configuration information.

Web browsers:

- Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway manager. The Content Gateway manager supports the following Web browsers:
  - Microsoft Internet Explorer 8, 9, 10, and 11
  - Mozilla Firefox versions 5 and later, except version 11 (due to an error in the way version 11 handles importing certificates)
  - Google Chrome 13 and later

> **Note**
> Browser restrictions apply only to the use of the Content Gateway manager and not to client browsers proxied by Content Gateway.

About upgrades

- Content Gateway upgrades from v7.7.x to v7.8.x require an additional step to avoid possible latency issues sometimes caused by scanning using async mode.
  1. Versions older than v7.7.x should first upgrade to v7.7.x.
  2. Download and install v7.7.x Hotfix 94. This hotfix adds background variables that retain sync mode.
  3. Upgrade from v7.7.x to v7.8.x. Sync mode is retained.
- When upgrading from 7.7.x, customized error message pages are lost. Record your customizations in advance and be prepared to reapply them after upgrade.
- If upgrading from a version prior to 7.8.2 and Allow Query Destination has been enabled and IP addresses are being logged, domain names will be logged after

upgrade. A variable was added and enabled in 7.8.2 that allows domain names to be logged when Allow Query Destination is enabled. (See Reducing DNS Lookups in Content Gateway Manager Help for more information.)

Instructions for downloading the installer

> **Note**
> If Content Gateway is running on a V-Series appliance, it is installed during factory imaging and upgraded when the v7.8.4 patch is applied. You do not need to download the installer.

To download the Content Gateway v7.8.4 installer:

1. Go to mywebsense.com and log in to your account.
   You are taken to the My Products and Subscriptions page.
2. Click the **Downloads** tab.
3. Under **Download Product Installers**, select your **Product and Version** (7.8.4).
   The available installers are listed under the form.
4. Click the plus sign ("+") next to an installer entry for more information about the installer.
5. Click the **download** link to download the installer.

Operating tips

Topic 60118 | Web Security Gateway and Gateway Anywhere | 26-Aug-2014

- *Installation*
- *Configuration*
- *IWA support for load balanced environments*
- *Proxy user authentication*
- *SSL Internal Root CA*

Installation

Software installation location and file ownerships

Content Gateway is installed in **/opt/WCG**.

Files are installed with **root** ownership.

Content Gateway processes are run as **root**.

Internet connectivity

It is recommended that the Content Gateway host computer have Internet connectivity before starting the software installation procedure. The software will install without Internet connectivity, but analytic databases cannot be downloaded from the Websense Database Download Server until Internet connectivity is available.

Ports

A full deployment of Content Gateway requires that several ports be open. See Installing Content Gateway in the Deployment and Installation Center for information about open ports and the reassignment of ports, if necessary.

Cluster handling during upgrades

Content Gateway tolerates different software versions in the same cluster. This is intended to simplify the process of upgrading a cluster. You should not run a cluster containing different versions for a prolonged period of time (many days).

Support for multiple versions in a cluster has these features and limits:

- Configuration synchronization does **not** take place among nodes of different versions.
- Condition alarms are passed among all nodes.
- The VIP feature is supported.

‘admin’ password restrictions

The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower-case letter, number, special character.

The password **cannot** contain the following special characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Cache size

Cache size should be restricted to 147 GB. This size provides optimal resource utilization while also providing an excellent end-user experience. Because today’s Internet sites are often composed of dynamic, uncacheable content, caching is a less significant factor in the end user’s Web browsing experience.

Configuration

In explicit proxy deployments, send HTTPS traffic to port 8080

In explicit proxy deployments, when HTTPS (SSL support) is enabled, client browsers should be configured to send HTTPS traffic to proxy port 8080.

Accessing Intranet sites in an explicit proxy deployment

If your clients cannot access your Intranet sites, verify that your operating system has been correctly configured to resolve all internal and external hostnames. Use the **nslookup** command to verify that a domain is listed in your DNS server:

For internal-facing servers:

```
nslookup intranet.example.com
```

For external Web sites:

```
nslookup www.example.com
```

If your organization has multiple DNS domains, verify that a hostname in each domain resolves correctly. If you are unable to resolve hostnames, verify the contents of the **/etc/resolv.conf** file, which provides search rules for how domain names are resolved in DNS.

When Content Gateway is on a V-Series appliance, the domain of the hostname is automatically added to **/etc/resolv.conf**. For example, if the hostname of the appliance is vseries.example.com, then Content Gateway treats “intranet” requests as “intranet.example.com”.

DNS proxy caching

The DNS proxy caching option allows Content Gateway to resolve DNS requests on behalf of clients. This option off-loads remote DNS servers and reduces response times for DNS lookups. You can use the DNS proxy caching option only with a layer 4 switch or a Cisco router running WCCP v2.

DNS proxy caching can only answer requests for A and CNAME DNS entries. Other types of request (e.g., MX) will not be answered.

Limitation: If the host name to IP address mapping is not in the DNS cache, Content Gateway contacts the DNS server specified in the **/etc/resolv.conf** file. **Only the first entry in resolv.conf is used.** This might not be the same DNS server for which the DNS request was originally intended.

See “DNS Proxy Caching” in Content Gateway Manager Help.

If your environment is configured such that you have DNS servers that resolve internal sites only and others that resolve external sites only, see Using the Split DNS option in Content Gateway Manager Help.

Virtual IP address must not match any real IP address

When configuring the Virtual IP feature, make sure that the Virtual IP addresses do not conflict with any existing IP addresses in the network.

Restart the proxy after protocol settings change

Any time you change your protocol settings in Content Gateway Manager (for example, with **Configure > SSL > Decryption/Encryption > Inbound > Protocol Settings**), you must restart the proxy for the new settings to take effect.

Using extended event logging

To investigate unexpected system behavior, it is sometimes helpful to enable the **Log Transaction and Errors** option (extended event logging) in Content Gateway Manager (**Configure > Subsystems > Logging**). However, extended event logging adds significant load to Content Gateway processes. Therefore you should **not** enable extended event logging when Content Gateway is at the high end of its processing capacity.

Reverse proxy

Content Gateway does **not** function as a reverse proxy.

IWA support for load balanced environments

Although IWA with a load balancer is supported in custom configured v7.7.3 deployments (Websense Technical Support assisted in these configurations), IWA with a load balancer is not supported in v7.8.1. Support is again provided, starting in v7.8.2.

> **Important**
> After upgrade to v7.8.4 check and, if necessary, rejoin IWA domains.

With Websense Content Gateway, Integrated Windows Authentication (IWA) uses the Kerberos protocol, with NTLM fallback.

In a load balanced environment, because the clients point to a FQDN that does not match the Content Gateway hostname, they receive a Kerberos ticket that Content Gateway cannot decrypt.

Normally, Content Gateway would be configured to share the hostname of the load balancer, but this is not possible when the load balancer requires hostname resolution (as with DNS-based load balancing).

In these cases, Content Gateway must be configured to use a custom keytab that corresponds to the load balancer's hostname for decryption.

Samba's implementation of Kerberos prevents this, because it requires keytab entries to match the service's hostname.

Starting in v7.8.2, this can be addressed with a 3-step solution.

> **Important**
> If your Content Gateway instances reside on a Websense appliance, contact Websense Technical Support for assistance with this procedure.

- **Step 1**: Add the custom SPN to the Kerberos domain (Active Directory) under the account object that Content Gateway used to join the domain.

  You can use the following command at the Windows command prompt:

  ```
  setspn -A <SPN> <content_gateway_hostname>
  ```

- **Step 2**: Edit the **keytab principals** parameter in **smb.conf**.

The parameter's value specifies a custom SPN entry. Samba rejects SPN entries that do not match the hostname of the service server.

The Kerberos decryption process now also matches against the custom SPNs in smb.conf, in the case that default matching fails.

Specify the custom SPN in smb.conf as follows:

```
keytab principals = HTTP/<custom SPN>.<domain>@<JOINED
REALM>
```

This prompts Content Gateway to attempt decryption with a keytab entry that matches the above hostname.

You must restart Content Gateway for the change to go into effect.

- **Step 3**: Add the keytab entry via Samba.

  The parameter in the file smb.conf enables the use of a specific custom SPN, but the Samba update is necessary to complete the configuration.

  1. To create a custom SPN entry in the keytab file, navigate to:

     ```
     /opt/WCG/contrib/samba/jails/<joined realm>
     ```

  2. Enter the **chroot** command.
  3. Run the following command:

     ```
     net ads keytab add <custom SPN>@<joined realm> -U
     <domain user>
     ```

     A password prompt appears. If authentication is succesful, the custom SPN is added into the keytab file.
  4. Windows caches clients' authentication. To ensure that all previous authentication is cleared, restart any clients that might have connected before this change was made.

Note that if the Content Gateway machine leaves and rejoins the domain, /opt/WCG/contrib/samba/jails/<joined realm> gets wiped and recreated, so Samba must be reconfigured.

Proxy user authentication

Client browser limitations

Not all Web browsers fully support transparent user authentication (prompt-less).

The following table indicates how a browser responds to an authentication request when Integrated Windows Authentication (IWA) is configured.

Browser/ Operating System	Internet Explorer (v10, 11 tested)	Firefox	Chrome	Opera (v12.02 tested)	Safari (v6.02 tested)
Windows	Performs transparent authentication	Performs transparent authentication (v28 tested)	Performs transparent authentication (v34, 35 tested)	Falls back to NTLM and prompts for credentials	Falls back to NTLM and prompts for credentials
Mac OS X	Not applicable	Performs transparent authentication (v28 tested)	Browser issue prevents IWA from working (v34, 35 tested)	Not tested	Performs transparent authentication
Red Hat Enterprise Linux, update 6	Not applicable	Performs transparent authentication (v28 tested)	Browser issue prevents IWA from working (v34,35 tested)	Not tested	Not applicable

LDAP support for passwords with special characters

LDAP user authentication can support passwords containing special characters.

Configuration is made directly in the **records.config** file.

The following parameter must be enabled, and the correct encoding name to which the special characters belong must be configured.

Add these entries to **records.config**. Note that the default setting is 0 (feature disabled).

```
// To enable the feature specify 1.
CONFIG proxy.config.ldap.proc.encode_convert  INT <1 or 0>
// Specify an encoding name here. For example,
// for German specify "ISO-8859-1".
CONFIG proxy.config.ldap.proc.encode_name  STRING <encoding
name>
```

SSL Internal Root CA

It is strongly recommended that all instances of Content Gateway use the same Root CA, and that for best security the signature algorithm be SHA-2, although SHA-1 is supported.

The default Root CA (presented to clients) is signed with SHA-256.

The best practice is to replace the Websense default Root CA with your organization's Root CA signed by SHA-2 or stronger. See Internal Root CA in Content Gateway Help.

The Root CA should be imported into all affected clients.

> **Note**
>
> Client connections may fail (depending on specific browser behavior) if the client sees a certificate generated by an unknown Root CA.

Post Upgrade: Data Security

If Web Security Gateway Anywhere and Data Security are deployed together and upgraded from v7.7.x to version 7.8.x, you must remove stale entries of Content Gateway instances registered in Data Security system modules:

1. Log onto the TRITON console.
2. Select the **Data Security** tab.
3. Select **Settings > Deployment > System Modules**.
4. There are 2 entries for each Content Gateway module registered with the system. Delete the older instances. You can identify these by looking at the version number.
5. Click **Deploy**.

If Web Security Gateway Anywhere and Data Security are deployed together and configured to use the on-box policy engine, and then reconfigured during upgrade or later to use the ICAP interface, the Content Gateway instance must be deleted from the list of Data Security system modules or the deployment will fail.

1. Log on to the TRITON console.
2. Select the **Data Security** tab.
3. Select **Settings > Deployment > System Modules**.
4. Locate the entry for the Content Gateway instance, click on it to open its **Details** page and then click **Delete**.
5. Click **Deploy**.

Resolved and known issues

Topic 60119 | Web Security Gateway and Gateway Anywhere | 26-Aug-2014

A list of resolved and known issues in this release is available to customers with a current MyWebsense account.

If you are not currently logged in to MyWebsense, the link takes you to a login prompt. Log in to view the list.